

Accès réseau Zero Trust

Les solutions Zero Trust de Cloudflare, notamment Access, améliorent la productivité des équipes et réduisent les risques, car tous les utilisateurs accèdent à vos applications auto-hébergées, SaaS ou non web sans passer par un VPN.

Un accès simple et sécurisé pour le travail hybride

Un accès réseau Zero Trust (ZTNA) natif d'Internet

L'environnement de travail distribué d'aujourd'hui exige une approche distribuée de la sécurité. Le « périmètre » n'existe plus et les solutions d'accès à distance traditionnelles, comme les VPN, ne peuvent répondre aux attentes modernes en matière de sécurité ou de performances.

Le ZTNA assure un accès simple et sécurisé entre n'importe quel utilisateur et n'importe quelle application, sur n'importe quel appareil et dans n'importe quel endroit, en contrôlant en permanence le contexte détaillé, comme l'identité et le niveau de sécurité des appareils, ressource par ressource. Grâce à notre approche entièrement nouvelle, vous n'aurez plus à « jouer les équilibristes » entre la sécurité et l'expérience utilisateur. Le ZTNA offre à votre entreprise tous les outils nécessaires pour améliorer les deux.

Il permet également aux entreprises d'être plus agiles et de mieux faire face aux changements, qu'il s'agisse de migration cloud, de fusions-acquisitions ou d'innovations et d'évolutions rapides. Cloudflare constitue le cœur d'une stratégie Zero Trust ou de modernisation de la sécurité, en proposant le ZTNA via sa connectivité cloud mondiale et programmable.

80% des clients ont constaté une réduction moyenne du temps passé à résoudre des tickets de support liés à l'accès à distance via un VPN.[1]

72% des clients ont économisé du temps sur la configuration mensuelle des politiques par rapport à leur fournisseur précédent.[1]

68% des clients ont remarqué un effet significatif concernant la rationalisation de l'expérience d'authentification des collaborateurs et de leurs sous-traitants.[1]

Redonnez le contrôle à votre entreprise grâce à un accès modernisé



Améliorez l'expérience utilisateur

Renforcez la productivité de vos équipes grâce à une sécurité modernisée qui rend les applications sur site tout aussi simples à utiliser que les applications SaaS. Dites au revoir aux VPN lents et encombrants ou aux plaintes de vos collaborateurs.



Mettez fin aux mouvements latéraux

Jugulez les risques informatiques et réduisez votre surface d'attaque en accordant un accès basé sur le contexte et le principe du moindre privilège plutôt qu'un accès au niveau du réseau, et ce pour chaque ressource.



Faites évoluer votre plateforme Zero Trust sans effort

Améliorez votre efficacité technologique en protégeant vos applications essentielles ou les groupes d'utilisateurs les plus à risque, avant d'étendre le ZTNA natif d'Internet à l'ensemble de votre entreprise.

Principaux scénarios d'utilisation d'Access

Sécurisation du travail hybride


Amélioration et remplacement du VPN : la solution Access est plus rapide et plus sûre que les VPN traditionnels. Commencez par décharger vos applications essentielles pour plus de sécurité et une meilleure expérience pour l'utilisateur final.


Accès des sous-traitants : authentifiez les utilisateurs tiers (comme les sous-traitants) grâce à des options sans client, des fournisseurs d'identité sociale et à bien d'autres fonctionnalités.

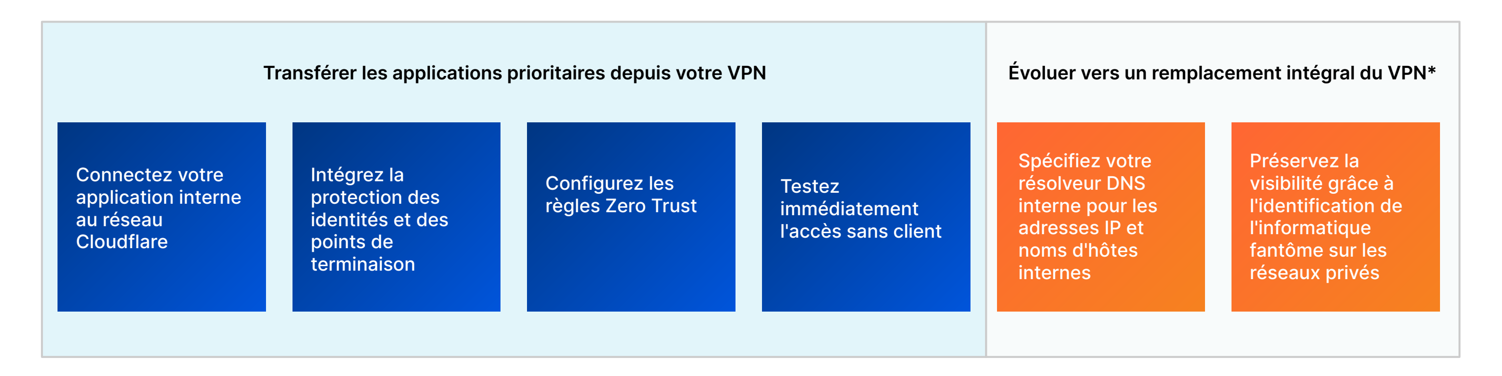
- **Accès des développeurs** : assurez à vos techniciens qualifiés un accès sécurisé à votre infrastructure essentielle sans compromis sur les performances.

Favorisez la modernisation numérique

- **Accélération des fusions/acquisitions** : évitez totalement les fusions de réseaux traditionnelles. Intégrez plusieurs fournisseurs d'identité et assurez un accès interne par application pendant le processus de fusion/acquisition.
- **Migration cloud** : assurez la continuité de l'activité lors des périodes de transformation, comme la migration des applications ou des répertoires d'identité vers le cloud.
- **Authentification MFA résistante au phishing** : déployez une authentification forte (comme des clés de sécurité conformes à la norme FIDO2) partout où vous le souhaitez.

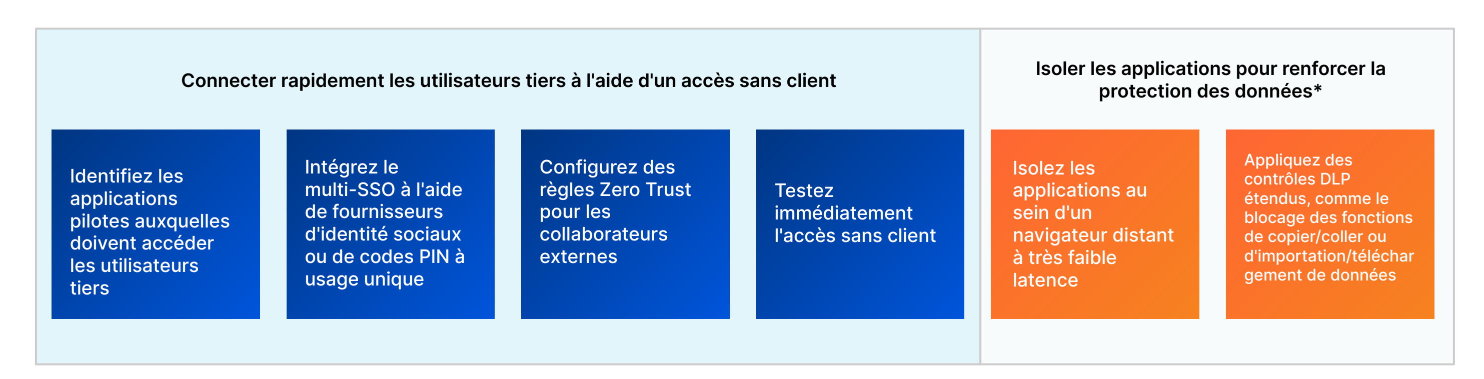
Premiers pas vers l'amélioration et le remplacement du VPN

Priorisez les applications essentielles ou les utilisateurs à risque grâce à un programme pilote ZTNA, en complément de votre VPN. Utilisez un accès sans client pour les applications web ou le SSH au sein d'un navigateur pour accélérer les tests. Adoptez les fonctionnalités avancées au fil du temps afin de progresser vers le remplacement total du VPN et de maintenir une visibilité dynamique pendant la transformation de votre réseau.



Premiers pas pour la mise en place d'un accès sous-traitants (tiers)

Proposez une expérience utilisateur fluide, tout en réduisant les risques liés aux appareils non gérés. Configurez des options d'authentification simples pour les sous-traitants, sans équipement logiciel requis au niveau de l'utilisateur final. Adoptez les fonctionnalités avancées au fil du temps pour une protection des données supplémentaire.



** À l'aide de fonctionnalités provenant d'autres parties de la plateforme Zero Trust*

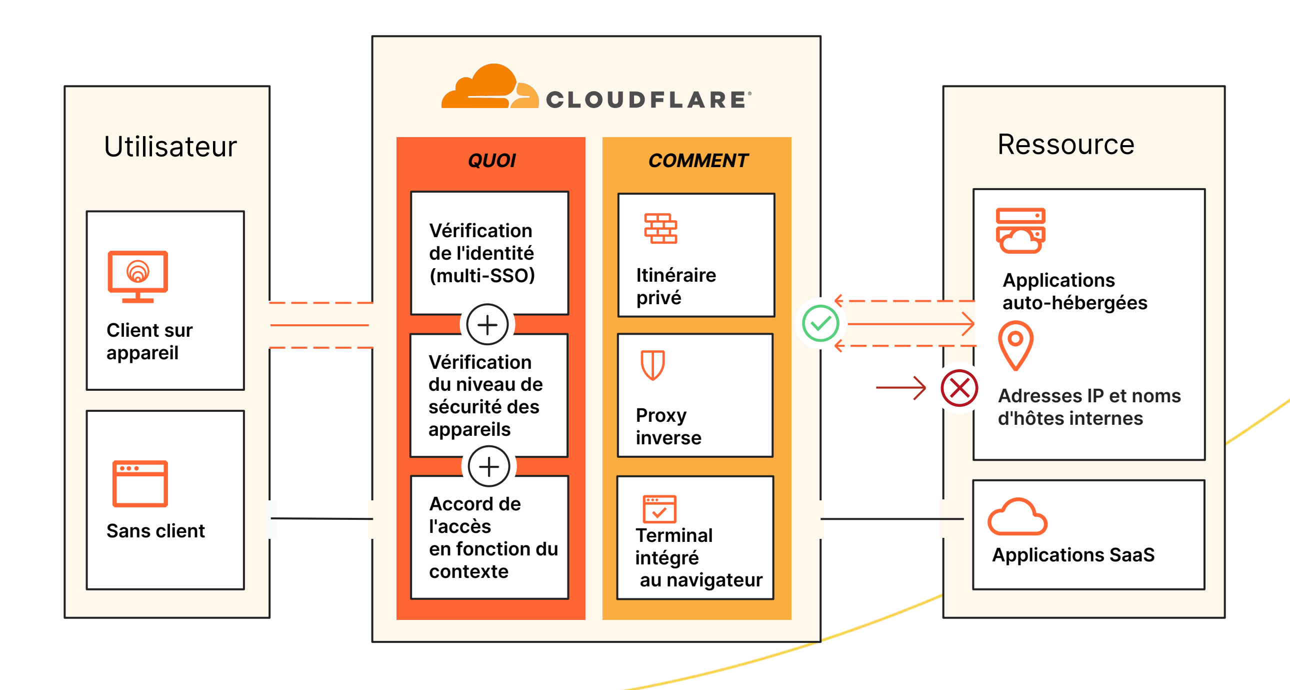
Comment fonctionne Access

Cloudflare Access est une couche d'agrégation flexible qui contrôle en permanence le contexte détaillé, comme l'identité et le niveau de sécurité des appareils afin de proposer un accès simple, sécurisé et individuel à l'ensemble des ressources d'une entreprise, de manière à créer un périmètre défini par logiciel. Lorsqu'un utilisateur s'authentifie et remplit tous les critères de la politique d'accès, le service Access émet un Web Token JSON signé, valable pour une durée de session spécifiée. Nous effectuons une inspection en une seule passe sur l'ensemble des requêtes des utilisateurs qui passent par notre plateforme composable. En outre, notre environnement d'administration de politiques centralisé propage les modifications des politiques en quelques secondes, grâce à l'architecture unique de notre réseau Anycast.

Notre système unifié avec et sans client gère tous les types d'appareils. Nous utilisons un client sur appareil unique pour l'ensemble des services Zero Trust. Ce dernier chiffre le trafic vers notre réseau afin de préserver la confidentialité des données de nos clients. Nous proposons également un accès simple et sécurisé aux appareils situés hors de la sphère de l'entreprise via notre configuration sans client. Nos excellents services d'accès réseau Zero Trust, de DNS, de pare-feu WAF et de protection contre les attaques DDoS fonctionnent en synergie afin de créer et de sécuriser des noms d'hôtes publics accessibles aux utilisateurs tiers et à nos collaborateurs en travail hybride, sur n'importe quel appareil. Nos options d'authentification sans utilisateur (jetons ou certificats mTLS) prennent également en charge les scénarios d'utilisation impliquant des services automatisés et des appareils IdO.

Concernant les mesures de contrôle Zero Trust, les ressources utilisent des noms d'hôte publics pour le proxy inverse vers les applications auto-hébergées (cloud/sur site) ou le SSH/VNC au sein d'un navigateur, le proxy d'identité vers les applications SaaS, ou le routage privé basé sur client/tunnel via proxy de transfert de couche 4-7 vers n'importe quelle ressource web ou non web (p. ex., TCP/UDP arbitraire) au sein d'un sous-réseau privé. L'association de notre réseau mondial et de notre connecteur d'applications logiciel prend en charge n'importe quel environnement de calcul (cloud public, dont Kubernetes et conteneurs ou ressources réseau sur site d'ancienne génération), sans nécessiter d'infrastructure VM et sans limites de débit, à la différence des autres fournisseurs de Zero Trust.

Les outils gérant les identités tierces, les points de terminaison, l'accès réseau direct (on-ramp), la journalisation/l'analyse et les SIEM sont intégrés à notre tableau de bord, en plus d'options natives pour notre client sur appareil et nos outils d'analyse, afin de permettre aux administrateurs de rester agiles et de travailler avec les outils qu'ils utilisent déjà.



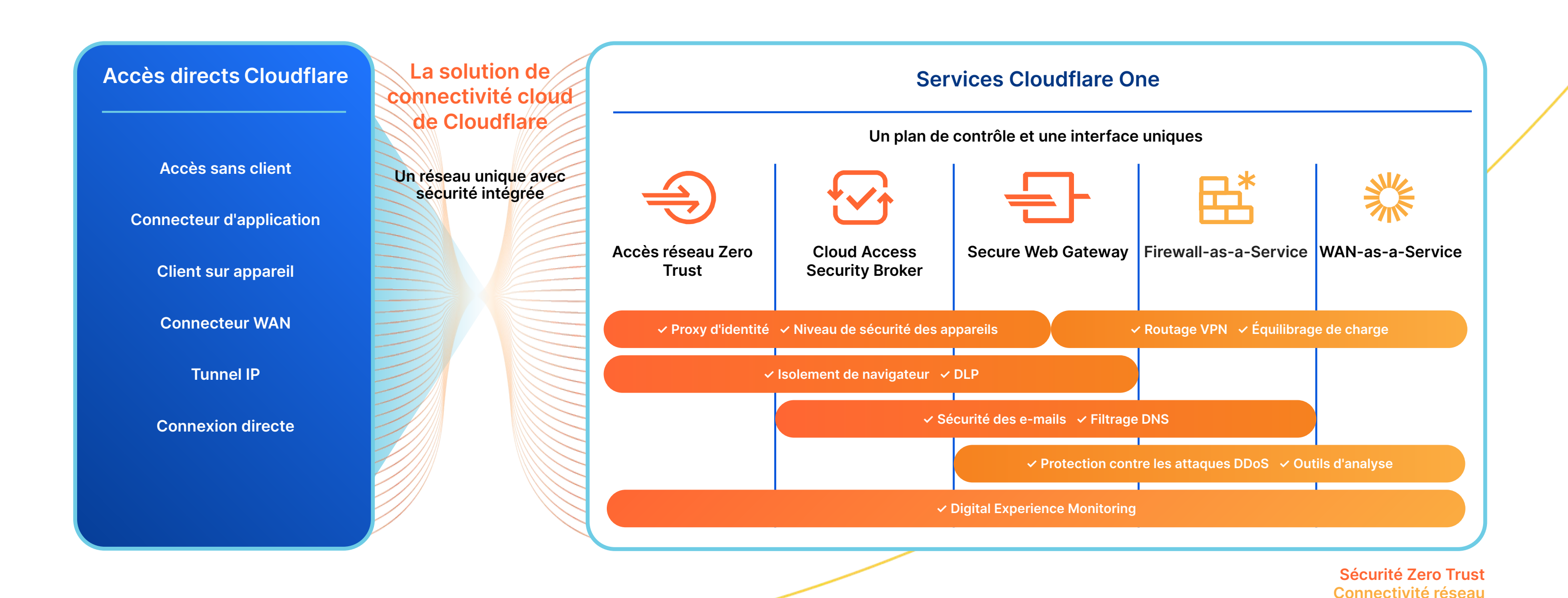
La solution Access en tant que composant de la plateforme SSE et SASE de Cloudflare

Tandis que le SSE et le SASE impliquent souvent un parcours stratégique de plusieurs années, Cloudflare voit fréquemment les entreprises se lancer sur la voie du ZTNA, car cette approche passe par des étapes réalisables et accessibles, tout en proposant une valeur considérable à court terme. Les dirigeants des services informatiques cherchent à sécuriser le travail hybride, à se défendre contre les menaces et à protéger les données au cours de leur parcours de consolidation. Dès lors, ils choisissent de plus en plus Cloudflare comme partenaire de confiance.

La flexibilité de déploiement et l'architecture composable de Cloudflare permettent à n'importe quelle entreprise de protéger et d'accélérer les performances de leurs appareils, de leurs applications et de réseaux tout entiers, afin de préserver la sécurité et la productivité du travail hybride. Pour ce faire, nous prenons en charge l'intégration sans agent pour les utilisateurs finaux, l'isolement web sans client pour contenir le trafic non sécurisé et un tableau de bord de gestion unifié permettant une visibilité sur l'ensemble des services de sécurité et des services réseau, indépendamment de l'endroit d'où les administrateurs ou les utilisateurs se connectent. L'étendue du réseau mondial de Cloudflare permet d'appliquer la sécurité à proximité des utilisateurs finaux, afin de minimiser la latence et de proposer une expérience fluide aux collaborateurs. Notre architecture Anycast nous aide à contourner les perturbations d'Internet, afin de préserver la présence en ligne des équipes et d'assurer la continuité de l'activité.

Avec notre plateforme SSE et SASE unifiée, le contexte partagé entre nos politiques ZTNA, CASB, DLP et SWG contribue à renforcer la stratégie de sécurité, tout en simplifiant la mise en œuvre grâce à des procédures d'administration cohérentes. Les mêmes attributs relatifs à l'identité et au niveau de sécurité des appareils peuvent informer à la fois les politiques d'accès du ZTNA et du CASB, ainsi que les politiques SWG, afin de simplifier la gestion des politiques entre les entreprises.

Les services de ZTNA, de RBI et de sécurité du courrier électronique peuvent être utilisés de manière conjointe afin de proposer un accès conditionnel aux ressources, tout en isolant les utilisateurs du contenu malveillant (liens, pièces jointes) auquel ils sont exposés sur leurs outils e-mail et leurs outils collaboratifs. Les sous-traitants et les utilisateurs situés sur des appareils non gérés peuvent se voir proposer un accès limité aux ressources de l'entreprise, les interactions de l'utilisateur (p. ex. importation/téléchargement, copier/coller, frappes clavier) étant désactivées afin d'empêcher la compromission des données. D'autres politiques DLP de couche 7 peuvent également être appliquées pour détecter les données sensibles.



Ce que nos clients en disent

« Cloudflare Access offre une alternative fantastique aux VPN traditionnels. Il suffit aux utilisateurs d'ouvrir leur navigateur et de se connecter, sans devoir télécharger ou configurer un logiciel supplémentaire. »

— **Platzi**, Head of Cloud Engineering

« La solution Access est bien plus simple et sécurisée qu'un VPN concernant la limitation de l'accès aux ressources internes. Il suffit de l'activer et d'ajouter des utilisateurs. Elle fonctionne, tout simplement ! »

— Bitpanda, CTO et confondateur

« Nous avons découvert la solution Cloudflare Access juste à temps pour nous empêcher de nous lancer dans la procédure compliquée de déploiement d'un VPN. Le choix s'est révélé particulièrement facile pour nous et Access s'est montrée incroyablement simple à déployer. »

— **ezCater**, Head of Security

« Avant le déploiement de Cloudflare, la préparation d'une application en vue de son déploiement était un projet de deux à quatre semaines. Cloudflare Zero Trust nous offre un gain de temps de près de 90 %. »

— **Creditas**, Network Engineering Team Lead

Ce qu'en disent les analystes



Cloudflare a été désignée comme Leader dans l'IDC MarketScape for Zero Trust Network Access (ZTNA) 2023

IDC cite la « stratégie de produits agressive de Cloudflare, qui aspire à répondre aux besoins des entreprises en matière de sécurité ». Nous pensons que cette reconnaissance valide notre approche consistant à aider les entreprises de toute taille à déployer l'architecture Zero Trust et à sécuriser l'accès de tous les utilisateurs à toutes les ressources, sans VPN.



Cloudflare a été désignée comme Leader dans le KuppingerCole Leadership Compass for ZTNA 2022

Dans son analyse du marché du ZTNA 2022, la firme KuppingerCole Analysts AG a cité plusieurs forces de Cloudflare, comme notre plateforme de sécurité totalement intégrée et développée de manière organique, notre vaste infrastructure cloud mondiale et notre gigantesque présence sur le marché.



Fonctionnalités d'Access

Créer/modifier des politiques Zero Trust pour l'accès sécurisé	
Politiques d'accès précises, personnalisées	Environnement d'administration de politiques centralisé. Les applications de couche 7 sont sécurisées au niveau du sous-domaine et du chemin grâce à la prise en charge des caractères génériques et des noms d'hôtes multiples. Nous prenons également en charge les requêtes CORS. Les modifications des politiques sont propagées en quelques secondes. La solution inclut un outil de test des politiques.
Étendue des ressources : ce que nous pouvons protéger et comment	Les ressources utilisent des noms d'hôte publics pour le proxy inverse vers les applications auto-hébergées (cloud/sur site) ou le SSH/VNC au sein d'un navigateur, le proxy d'identité vers les applications SaaS, ou le routage privé basé sur client/tunnel via proxy de transfert de couche 4-7 vers n'importe quelle ressource web ou non web (TCP/UDP) au sein d'un sous-réseau privé.
Identité	Authentification via l'ensemble des grands fournisseurs d'identité (IDP) d'entreprise et sociaux, y compris avec plusieurs IdP simultanés. Peut également utiliser les connecteurs génériques SAML et OIDC. La solution prend en charge (et peut faire appliquer) n'importe quelle méthode d'authentification proposée par un IDP, l'authentification temporaire, la justification de finalité, les intervalles de réauthentification à l'échelle mondiale ou par session, et une option de révocation de session immédiate pour chaque application ou chaque utilisateur.
Niveau de sécurité des appareils	Contrôle du niveau de sécurité des appareils à l'aide d'un client sur appareil et d'intégrations à une plateforme de protection des points de terminaison (Endpoint Protection Provider, EPP) tierce. Utilisation d'intégrations service à service pour incorporer les scores de risque EPP aux politiques Zero Trust.
Signaux contextuels pour les politiques	Configuration de signaux, comme le groupe d'e-mails, les plages IP, la géolocalisation, la méthode de connexion (p. ex., type de MFA, type d'IDP), le certificat mTLS ou SSH valide, le jeton de service, la liste des numéros de série, les attributs du niveau de sécurité des appareils, l'installation d'un client sur appareil, la durée de session, l'application de règles SWG ou des signaux provenant d'appels d'API externes. La solution peut également consulter directement les politiques d'accès conditionnel Microsoft Entra ID (Azure AD).
Autres fonctionnalités connexes prises en charge	• **SCIM :** provisionnez/déprovisionnez automatiquement les utilisateurs pour les applications auto-hébergées et SaaS (exemples pour Okta et Azure AD). • **DNS interne :** configurez la connexion de secours sur le domaine local et résolvez les requêtes transmises au réseau privé. • **Tunnellisation fractionnée :** incluez/excluez des adresses IP pour les réseaux privés ou pour l'exécution en complément d'un VPN. • **Authentification mTLS :** authentification basée sur certificat pour l'IdO et les autres scénarios d'utilisation du mTLS. • **Isolement des applications :** en cochant une simple case, isolez les applications au sein de notre navigateur à distance ultrarapide*.
Accès on-ramps et off-ramps (rampes directes d'accès et de sortie)	
Connecteur d'application	Orchestration simple de notre connecteur d'applications léger (Cloudflare Tunnel) qui accélère la connexion des ressources à Cloudflare, sans nécessiter d'infrastructure VM et sans limites de débit. Inclut des fonctionnalités de surveillance, de réseaux virtuels (pour les chevauchements d'IP), ainsi que de redondance et de basculement.
Client sur l'appareil : à quel moment l'utiliser	• **Sans client :** élargissez les politiques Zero Trust aux utilisateurs tiers sur des appareils non gérés. Cette approche s'associe bien au RBI sans client et aux politiques DLP de couche 7*. L'accès sans client prend en charge les applications web et le SSH/VNC au sein d'un navigateur. • **Accès basé sur client :** notre client sur appareil (Cloudflare WARP) étend l'accès sécurisé aux réseaux privés, permet les intégrations de niveaux de sécurité des appareils service à service. Il est également sensible à la régionalisation afin d'appliquer des politiques sur mesure aux utilisateurs sur site. La solution peut aussi connecter deux appareils exécutant WARP ou plus pour créer des réseaux privés. Les utilisateurs peuvent effectuer une auto-inscription ou procéder au déploiement via MDM.
Extensibilité et visibilité	
Personnalisation des pages	Importez du HTML personnalisé pour vos pages de blocage et de lancement d'applications afin de les faire correspondre à votre image de marque ou de véhiculer des instructions d'accès spécifiques afin de rationaliser l'expérience de l'utilisateur final.
Journalisation	Journalisation complète pour l'ensemble des requêtes, des utilisateurs et des appareils. La solution peut utiliser logpush ou une API pour s'intégrer aux outils existants en matière de SIEM, d'orchestration et d'analyse. Pour les ressources inconnues, notre Shadow IT pour l'infrastructure interne catalogue de manière passive le trafic unique afin de faire apparaître toutes les origines.
Automatisation	Des API intuitives et un fournisseur Terraform sont disponibles pour gérer tous les aspects d'un déploiement Zero Trust de manière programmatique. La solution propose également la prise en charge des jetons de service sans utilisateur pour les services automatisés.

** À l'aide de fonctionnalités provenant d'autres parties de la plateforme Zero Trust*

Pourquoi choisir Cloudflare ?



Simplicité de configuration et de gestion

Simplifiez radicalement la configuration et la circulation du trafic en accès direct vers des ressources privées grâce à un connecteur d'applications logiciel et à l'orchestration des tunnels.



Expérience fluide et toujours active

Bénéficiez de performances supérieures pour les utilisateurs finaux et d'une résistance de premier ordre aux pannes du réseau grâce à la technologie Anycast mondiale de Cloudflare, qui vous assure la fiabilité dont vous avez besoin.



Innovations rapides, axées sur l'adoption précoce

Suivez les évolutions du réseau Internet lui-même grâce à un fournisseur qui surclasse constamment ses pairs en termes d'innovations afin de rendre l'accès aux applications plus rapide et plus sécurisé.

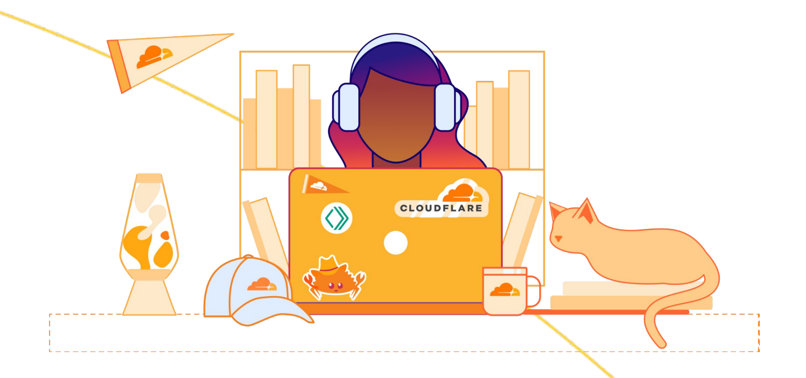
Discutons d'un accès simple et sécurisé pour votre entreprise

Demander un atelier



Vous n'êtes pas encore prêt à avoir une discussion en direct ?

Cliquez ici si vous souhaitez continuer à en apprendre davantage sur la plateforme SSE et SASE de Cloudflare



1. Étude 2023 : techvalidate.com/product-research/cloudflare/charts